



SECURITY AGREEMENT LACDMH USER

It is the policy of the County of Los Angeles and the Department of Mental Health (LACDMH) that each County employee, whether permanent, temporary, part-time, contract, or in any other status, is individually responsible for the protection of all confidential applicant and participant information, as well as all County information, data, and information processing resources to which he or she has been provided access to.

As an LACDMH workforce member, you may have access to confidential mental health information about clients contained within LACDMH applications, systems, resources and DMH Electronic Health Record Systems. All LACDMH workforce members have an obligation to protect this sensitive information.

As a user of LACDMH System, I understand that my responsibilities include, but are not limited to, the following:

1. All sensitive information obtained from LACDMH systems and resources is confidential and shall not be disclosed to any unauthorized person(s) or group(s). If in doubt, I must consult with my immediate supervisor or manager.
2. I must always protect the privacy and confidentiality of LACDMH clients, and I acknowledge that data browsing is strictly prohibited.
3. I am responsible for the secrecy of my password. My password must neither be written down nor told to anyone. If I know or suspect that my password is known by someone other than myself, I must immediately change my password, and notify the Help Desk, my immediate supervisor or manager.
4. I am not permitted to allow any other person to logon or access DMH systems and resources using my password.
5. I may only use DMH systems and resources for those specific functions for which I am authorized. Personal, non-County business, and/or unauthorized use of LACDMH systems and resources are forbidden.
6. I understand that it is illegal for me to knowingly access LACDMH systems and resources to add, delete, alter, damage, destroy, copy or otherwise use the system to defraud, deceive, extort, or control data for wrongful personal gain.
7. I understand that my access to confidential information in all LACDMH systems and resources is logged and may be audited at any time.
8. I must dispose of documents or other media that are no longer needed using an LACDMH Chief Information Office Bureau (CIOB) approved method that protects confidentiality as documented in LACDMH Policy 554.01, Device and Media Control Policy.



9. Only data that I believe to be correct may be entered into LACDMH systems and resources. I am not to enter any data which I know or believe to be incorrect. I must notify my immediately supervisor, and if necessary, my chain of command, if I am ever requested to knowingly enter incorrect data.
10. I must Log-off from LACDMH systems and resources or lock and secure my workstation when unattended.
11. I am not permitted to copy, export, download, store, save, print or capture screen displays, photograph or video-graph data from LACDMH systems and resources without prior written authorization from LACDMH Departmental Privacy and Security Officers unless the action listed above is an approved part of conducting business as defined by my role.
12. I am not permitted to install, transmit, copy or download any software from or into LACDMH systems and resources without specific written authorization from LACDMH CIOB management.
13. I am not permitted to connect or disconnect any hardware or peripherals to or from LACDMH systems and resources without specific written LACDMH CIOB management authorization.
14. I must immediately report to my direct supervisor or manager any suspected violation of this LACDMH User Security Agreement, and/or any misuse or non-compliance with any LACDMH systems and resources operating standards and procedures.

I have read and understand this entire User Security Agreement and agree to abide by it. I recognize that my failure to fulfill these responsibilities, including the knowledge of anyone else using my password, could result in the abuse of County information resources and data, and that the County may hold me responsible for such abuse.

I further understand that any violation of this agreement may result in disciplinary action up to and including discharge. I also have been informed that failure to comply with Health Insurance Portability and Accountability Act of 1996 (HIPAA) can result in civil and criminal penalties per 42 USC § 1320d-5.

Workforce Member's Name

Workforce Member's Signature

Date

Business Associate / Contractor Approver: As a representative and liaison of the Non-LACDMH organization performing in a management or supervisory capacity, I certify that the above signer, whose conduct in the performance of work for accessing LACDMH resources is under my authority, has acknowledged and signed this Security Agreement.

Manager's Name

Manager's Signature

Date